Raspodijeljene glavne knjige i kriptovalute

Pristupi rudarenju i konsenzusu

Ante Đerek, Zvonko Konstanjčar

14. studenoga 2021.

Ponavljanje: Raspodijeljeni konsenzus - izazov

Idejno rješenje: treba nam mehanizam kojim ćemo birati slučajan čvor, ali tako da u barem 50% slučajeva izaberemo POŠTEN čvor.

Problem odabira poštenog čvora - motivacija - poticaji

- Nagrada za blokove
- Nagrada za transakcije

Dodatni problemi

- Možemo li zaista konstruirati robustan mehanizam za biranje slučajnog čvora
- Nagrade motiviraju sve čvorove da se uključe - mogu samo dobiti
- Napadači mogu kreirati *sybil* čvorove te preko njih "upravljati" konsenzusom

Ponavljanje: Raspodijeljeni konsenzus - izazov

Idejno rješenje navedenih problema: umjesto slučajnog čvora, biramo čvor proporcionalno resursima koje taj čvor posjeduje, uz uvjet da se ti resursi ne mogu monopolizirati.

Izvedbeno dva pristupa

- Ako je resurs računalna snaga - **proof-of-work** sustav (za sada je taj sustav implementiran u Bitcoinu)
- Ako je resurs posjedovanje valute - **proof-of-stake** sustav (za sada implementirane neke varijante, ali područje aktivnog istraživanja)

Ponavljanje: proof-of-work

Što znači odabir čvora proporcionalno računalnoj snazi koju taj čvor posjeduje?

Idejno rješenje: Pustiti da se čvorovi natječu koristeći njihovu računalnu snagu.

Kod Bitcoina

- proof-of-work je realiziran preko rješavanja kriptografskih slagalica
- Čvor koji predlaže blok mora pronaći broj (koji nazivamo *nonce*) takav da $H(nonce|hash_{prev}|x_1|x_2|\ldots|x_n) < t$, za neki unaprijed zadani prag t.

Ponavljanje: proof-of-work preko kriptografskih slagalica

Nužna svojstva slagalice

- **Teško ju je riješiti** - za Bitcoin u 2018., u prosjeku za pronaći jedan ispravan *nonce* treba ispitati 10^{22} opcija.
- **Ima podesivu težinu** - kod Bitcoina je to ostvareno preko parametra t, pravilo 10-minuta.
- **Jednostavna za provjeru** - kod Bitcoina kada se zna *nonce*, svi lagano mogu provjeriti da on zadovoljava zadanu težinu.

Definicija

Rudarenje je kontinuirani proces rješavanja slagalica, a čvorovi koji sudjeluju u tome nazivaju se rudari.

Ponavljanje: vrijednost Bitcoina

Bitcoin mreža je sigurna ako većina rudara otežana po hash snazi igra po pravilima, tj. poštena je.

Tri važne povezane ideje oko Bitcoina - cirkularna ovisnost

- Sigurnost sustava kriptovalute ovisi o rudarenju
- Rudarenje ovisi o vrijednosti kriptovalute
- Vrijednost kriptovalute ovisi o sigurnosti sustava

Danas..

Posao Bitcoin rudara

- Provjeravaju transakcije
- Izgrađuju i spremaju blokove
- Dogovaraju se koji će blok ići u lanac blokova

Pitanja za danas

- Tko su rudari?
- Zašto to rade?
- Kako to rade?
- Kakav im je poslovni model?
- Kakav im je utjecaj na okoliš?

Treba li ući u taj posao?

Aktivnosti Bitcoin rudara

Glavne aktivnosti rudara

- Osluškuju transakcije
- Održavaju lanac blokova i osluškuju nove blokove
- Sastavljaju nove blokove i traže *nonce*
- Prate status svog bloka
- Zarađuju

Dvije kategorije aktivnosti rudara

- **Validiraju transakcije i blokove** (primarni posao) - pomažu održavanju sigurnosti Bitcoin sustava
- **Utrkuju se u predlaganju blokova i tako zarađuju** (sekundarni posao) - nisu nužne za Bitcoin mrežu, ali motiviraju rudare da odrađuju primarni posao.

Sastavljanje ispravnog bloka

Osnovne aktivnosti

- Sakupljanje validnih transakcija, sami rudari biraju koliko, te organiziranje njih u Merkleovo stablo
- Izgradnja bloka s zaglavljem koje pokazuje na prethodni blok

Izvor: `bitcoinbook.cs.princeton.edu`

Sastavljanje ispravnog bloka

Potraga za *nonce* (32-bitna vrijednost)

- *nonce* u zaglavlju bloka
- Dodatni *nonce* u coinbase transakciji

Izvor: `bitcoinbook.cs.princeton.edu`

Sastavljanje bloka

Zadatak

Rješavaju li svi rudari isti zadatak?

Zadatak

Postoji li rješenje zadatka?

Određivanje težine sastavljanja bloka

Promjena nakon svakih 2016 blokova

- $t_{n+1} = \frac{t_n \cdot 2016 \cdot 10\text{minuta}}{T_n}$, gdje je T_n vrijeme potrebno za rudarenje zadnjih 2016 blokova
- Svaki rudar računa nezavisno težine t_n i prihvaća blokove koji zadovoljavaju njegovu težinu
- Rudari koji rudare na različitim granama mreže, mogu rudariti s različitim težinama
- Promjena otprilike svaka dva tjedna

Izvor: `bitcoinbook.cs.princeton.edu`

Vrijeme sastavljanja bloka

2014. godina, izvor: `bitcoinbook.cs.princeton.edu`

2015. godina, izvor: `bitcoinbook.cs.princeton.edu`

Vrijeme sastavljanja bloka

2018. godina, izvor: `bitcoinwisdom.com/bitcoin/difficulty`

Hardver za rudarenje

Težak zadatak: kako bi se dobio hash, kod Bitcoina je potrebno napraviti dvostruki SHA-256 bloka.

- CPU (engl. Central Processing Unit)
  - Prvi rudari, u praksi se više ne koriste
  - Hashrate: $\propto 10^5$ (za Ethereum: $\propto 10^5$)
  - Kod današnjih težina trebalo bi u prosjeku nekoliko tisuća godina da se sastavi blok
- GPU (engl. Graphical Processing Unit)
  - Rudarenje je moguće paralelizirati
  - Hashrate: $\propto 10^8$ (za Ethereum: $\propto 10^7$)
  - Imaju dosta ugrađenog hardvera koji nije potreban za rudarenje - problem grijanja

Hardver za rudarenje

Neki naslovi

- Zagrebački vatrogasci: Znamo da je rudarenje 'in', ali evo kako preopterećenje instalacija može završiti, www.tportal.hr, 2018.
- Russian nuclear scientists arrested for Bitcoin mining plot, www.bbc.com, 2018.

Izvor: `bitcoinwisdom.com/bitcoin/difficulty`

Hardver za rudarenje

Market Summary > NVIDIA Corporation

289.36 USD

NASDAQ: NVDA

+151.79 (110.04%) ↑ past year

+ Follow

Nov 4, 11:19 EDT • Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

Open	272.29	Mkt cap	725.67B	CDP score	A-
High	290.88	P/E ratio	103.53	52-wk high	290.88
Low	271.18	Div yield	0.055%	52-wk low	115.66

Nvidia

Computer systems design services company

Nvidia Corporation is an American multinational technology company incorporated in Delaware and based in Santa Clara, California. It designs graphics processing units for the gaming and professional markets, as well as system on a chip units for the mobile computing and automotive market. Wikipedia

CEO: Jensen Huang (Apr 1993–)

Founded: April 1993

Headquarters: Santa Clara, California, United States

Revenue: 10.92 billion USD (2020)

Subsidiaries: Mellanox Technologies, DeepMap, Parabricks LLC, MORE

Izvor: `google.com`

Hardver za rudarenje

Izvor: `finance.yahoo.com`

Hardver za rudarenje

- FPGA (engl. Field Programmable Gate Array)
  - Oko 2011. godine neki rudari prelaze s GPU na FPGA
  - Bolje performanse od GPU, ali ne dovoljno
  - Imaju dosta ugrađenog hardvera koji nije potreban za rudarenje
- ASIC (engl. Application Specific Integrated Circuit)
  - Najbrži razvoj čipa u povijesti - od definicije problema do čipa
  - Mogu se birati modeli (razlike u cijeni, potrošnji energije, itd.)
  - Hashrate: $\propto 10^{13}$ (za Ethereum: $\propto 10^{8}$)
  - Kako se hash snaga mreže stabilizirala, oprema za rudarenje ima dulji vijek trajanja
  - Veći dio vremena zarada rudara je uglavnom dolazila od rasta vrijednosti Bitcoina, a ne od nagrada za rudarenje
- Profesionalno rudarenje
  - Detalji kako ti centri funkcioniraju nisu u potpunosti poznati - poslovna tajna
  - Tri ključna parametra za uspostavu centra: **klima, cijena struje, brzina mreže**

Evolucija rudarenja

Izvor: `bitcoinbook.cs.princeton.edu`

- Slična evolucija poslovanja - individualni rudari su s vremenom nestali (sav profit odlazi velikim centrima)
- U oba slučaja najviše su zaradili oni koji su prodavali opremu
- Strategija za male rudare - altcoini u ranim fazama

Energija i ekologija

- Landauerov princip (Ralph Landauer, 1960. god.)
  - Bilo koja nereverzibilna računarska operacija mora iskoristiti neki minimalan iznos energije
  - Brisanje bilo kojeg bita informacije troši $kT \ln 2$ J, $k = 1.3910^{-23}$ J/K Boltzmannova konstanta
  - Svaki put kada se bitovi okrenu na nereverzibilan način sigurno se troši neki minimum energije (električna energija prelazi u toplinu)
- Ugrađena energija (eng. embodied energy)
  - Energija potrebna za proizvodnju opreme za rudarenje
  - S vremenom sve manja - mreža postaje stabilnija
- Električna struja
  - Uvijek će trebati - Landauerov princip
  - Potrošnja pada kako ASIC sustavi postaju efikasniji
- Hlađenje
  - Veća potrošnja, ako se rudari u centrima
  - Energija u formi električne struje

Koliko energije troši Bitcoin mreža

- Top-down pristup
  - Svakih 10 min pronađe se jedan blok i rudari dobe nagradu od 6.25 BTC koji vrijede približno 387,500.00 USD
  - Otprilike 646 USD svake sekunde je stvoreno u Bitcoin ekosustavu i predano rudarima
  - Troškovi struje su oko 0.05 USD za 1 kWh (0.015 USD za 1 MJ)
  - Kada bi rudari sav novac trošili na struju tada bi uzimali iz mreže 43 GW (2015. godine to je bilo 0.37 GW)
- Bottom-up pristup
  - jedni od efikasnijih ASIC sustava za rudarenje rade na $10.8 GHash/s/W$
  - Hashrate mreže - $51.043 EHash/s$
  - Potrebno je oko 4.7 GW energije za taj broj hasheva po sec.

Koliko energije troši Bitcoin mreža

Izvor: `www.cbeci.org`

Koliko je GW energije

- Jedna od najvećih hidroelektrana proizvede - $10GW$
- Najveća nuklearna elektrana na svijetu proizvede - $7GW$
- Prosječna hidroelektrana proizvede - $1GW$, a nuklearka - $4GW$
- Ukupna godišnja potrošnja električne struje u RH - $18.35TWh$, što je ekvivalentno prosječnoj snazi $2.1GW$

Koliko energije troši Bitcoin mreža

Izvor: www.cbeci.org

Ekonomija malog rudara

- Bitcoin
  - Spremni ste investirati u Bitcoin rudarenje
  - Kupite ASIC (npr. Dragonmint 16T) - 3,500.00 USD
  - HashRate - $1.610^{13} \rightarrow u_x = 3.110^{-7}$
  - U prosjeku nalazimo 1 blok u 60 godina $\rightarrow \lambda = 1.6310^{-2}$ blokova/godini
  - Vjerojatnost da smo u godinu dana završili k blokova je $\frac{\lambda^k e^{-\lambda}}{k!}$

k	0	1	> 1
vjerojatnost	98.38%	1.6%	0.02%

Ekonomija malog rudara

- Ethereum
  - Spremni ste investirati u Ethereum rudarenje
  - Kupite GPU (npr. MSI Radeon R9 390X) - 500.00 USD
  - Hashrate - $2.9 \cdot 10^7$
  - U prosjeku nalazimo 0.25 blokova u godinu dana $\rightarrow \lambda = 0.25$ blokova/godini
  - U prosjeku godišnje zarađujemo 168 USD (ne računajući troškove struje).
  - Vjerojatnost da smo u godinu dana završili k blokova je $\frac{\lambda^k e^{-\lambda}}{k!}$

k	0	1	> 1
vjerojatnost	78%	19.5%	2.5%

Bazeni Bitcoin rudara

Zajedničko osiguranje malih rudara. Rudari udružuju resurse i formiraju bazen te zajedno traže odgovarajući *nonce*.

Bez obzira tko pronađe blok - manager bazena prima nagradu i raspoređuje ostalima.

Podjela zarade:

- Pay-per-share model - jednako za svaki hash koji zadovoljava neki uvjet
- Proporcionalan model - iznos ovisi je li bazen našao blok ili ne (ako da, onda zarada proporcionalna radu)

Bazeni Bitcoin rudara - podjela zarade

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
0000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E7776138456181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Izvor: `bitcoinbook.cs.princeton.edu`

Bazeni Bitcoin rudara - podjela zarade

Izvor: `bitcoinbook.cs.princeton.edu`

Bazeni Bitcoin rudara - distribucija hashratea

2014. godina, izvor: `bitcoinbook.cs.princeton.edu`

Bazeni Bitcoin rudara - distribucija hashratea

2015. godina, izvor: `bitcoinbook.cs.princeton.edu`

Bazeni Bitcoin rudara - distribucija hashratea

2018. godina, izvor: `www.blockchain.com`

Bazeni Bitcoin rudara - prednosti i nedostaci

Prednosti

- Smanjuju rizike i volatilnosti
- Mali rudari mogu se uključiti u posao
- Održavanje softvera mreže je jednostavnije - ipak neka razina centralnosti

Nedostaci

- **51 % napad** - nije lagano utvrditi tko je s kime povezan
- U načelu rudari mogu napustiti bazene, ali pitanje je kako to funkcionira u praksi
- Smanjuje se broj čvorova koji validiraju transakcije (tj. vrte kompletan softver)